ABSTRACT

A system and method for signing, sorting, and authenticating electronic documents using public key cryptography. The system comprises a document service computer cluster connected to user computers, document owner server computers, and registration computers via a network such as for example, the internet or the world wide web. Document owners and system users can store electronic documents in an encrypted database located on the document service computer cluster, or on a document safe connected to the document owner server. [Individuals register as users on registration computers and receive registration credentials. Users can access the system by browsing the world wide web using any commercially available browser running on a user computer, and by locating the document owner server computer, or by locating the document service web server in the document service computer cluster. Users can login to the system by entering appropriate credentials during login.] Users can sign documents by identifying the document to be signed and sending a signing request to the document service computer cluster. The document service computer cluster retrieves the user's private key, which is located securely in a database on the cluster, and signs the identified document. [A user can sign documents from any user computer having access to the web. The user's private key remains secure on the document service computer cluster at all times.] No dedicated signing software need be installed on the user computer prior to accessing the document service computer cluster.